(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 776 410**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **98 03471**

(51) Int Cl^6 : G 06 K 19/073, G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 20.03.98.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 24.09.99 Bulletin 99/38.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *GEMPLUS Société en commandite par actions* — FR.

(72) **Inventeur(s)** : NACCACHE DAVID, FEYT NATHALIE et BENOIT OLIVIER.

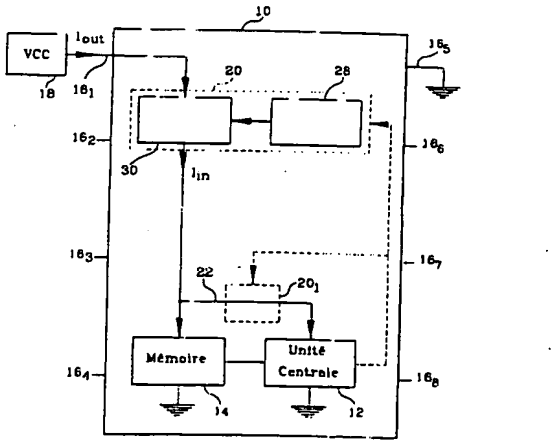
(73) **Titulaire(s)** :

(74) **Mandataire(s)** : GEMPLUS.

(54) DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR.

(57) L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte contre les intrusions frauduleuses par l'analyse du courant consommé.

L'invention réside dans le fait d'ajouter dans la carte un dispositif (20) qui modifie le courant consommé, soit en le moyennant par une intégration, soit en lui ajoutant des valeurs aléatoires par un générateur de signaux aléatoires (28) de manière à masquer les opérations effectuées. Dans une variante, il est prévu d'effectuer simultanément une opération à sécuriser et l'écriture dans une mémoire EEPROM, cette dernière créant des variations de courant chaotiques qui masquent l'opération à sécuriser.



FR 2 776 410 - A1

1

DISPOSITIFS POUR MASQUER LES OPERATIONS EFFECTUEES DANS UNE CARTE A MICROPROCESSEUR

L'invention concerne les cartes à microprocesseur et, dans de telles cartes, différents dispositifs pour masquer les opérations effectuées dans la carte dans le but d'améliorer la sécurité contre les intrusions frauduleuses.

Les cartes à puces se divisent en plusieurs catégories, à savoir :

- les cartes à simple mémoire,
- les cartes à mémoire dite carte intelligente, et
- les cartes à microprocesseur.

Une carte à simple mémoire permet d'effectuer des opérations de lecture et d'écriture dans la zone de mémoire morte électriquement effaçable de façon libre. Une telle carte est d'un faible coût mais elle ne présente pas une sécurité suffisante de sorte qu'elle est de moins en moins utilisée.

Une carte à mémoire intelligente améliore notamment la sécurité des opérations de lecture/écriture en les autorisant seulement lorsque certaines conditions réalisées sous forme câblée sont remplies.

Une carte de la troisième catégorie contient un microprocesseur capable d'exécuter des programmes enregistrés dans une mémoire et d'effectuer ainsi des calculs avec des données secrètes inaccessibles au monde extérieur à la carte. Ainsi, une clé enregistrée dans la mémoire peut servir à valider une transaction électronique telle qu'un achat ou une ouverture de porte sans avoir à être manipulée à l'extérieur de la carte.

Malheureusement, certains microprocesseurs présentent des consommations de courant qui dépendent des calculs effectués à l'intérieur de la carte. Ainsi, un calcul cryptographique comprenant une arborescence de calcul qui dépend des chiffres de la clé utilisée aura différentes empreintes de consommation de courant selon la valeur de la clé utilisée. Il en résulte qu'un fraudeur pourrait corréler l'empreinte de consommation de courant de la clé utilisée et ainsi remonter à la valeur de la clé.

Pour empêcher cette corrélation, une contre-mesure courante consiste à programmer l'algorithme cryptographique d'une manière telle que quelle que soit la valeur de la clé, l'algorithme passera toujours les mêmes étapes de calcul.

De nombreux algorithmes dits "orientés octets" se prêtent bien à ce mode de programme mais d'autres posent quelques problèmes techniques qui ne sont surmontables qu'au prix de performances calculatoires moins optimales.

La présente invention a donc pour but de mettre en oeuvre dans les cartes à microprocesseur des dispositifs pour masquer les opérations effectuées tout en permettant au programmeur le libre-choix des règles de programmation, qu'elles soient du type "orientées octets" ou non.

Ce but est atteint en modifiant ou brouillant la consommation de la carte de manière que son empreinte soit indépendante des calculs effectués.

Cette modification ou ce brouillage de l'empreinte peut être obtenue en ajoutant dans la carte un dispositif qui modifie la consommation de courant.

Dans un premier exemple de réalisation, ce dispositif consomme de la puissance électrique de

manière irrégulière ou aléatoire qui s'ajoute à celle de la consommation normale.

Dans un deuxième exemple de réalisation, ce dispositif réalise une consommation moyenne en réalisant, par exemple, une intégration du courant consommé.

Dans un troisième exemple de réalisation, ce dispositif déclenche le circuit de programmation ou d'effacement de la mémoire du microprocesseur qui consomme de la puissance de manière chaotique, puissance qui masque la consommation due aux opérations effectuées par le microprocesseur pendant la programmation ou l'effacement de la mémoire.

D'autres caractéristiques et avantages de la présente invention effectueront à la lecture de la description suivante d'exemples particuliers de réalisation, ladite description étant faite en relation avec les dessins joints dans lequels :

- la figure 1 est un schéma fonctionnel d'un premier exemple de réalisation de l'invention,
- la figure 2 est un schéma fonctionnel d'un deuxième exemple de réalisation de l'invention, et
- la figure 3 est un schéma fonctionnel d'un troisième exemple de réalisation de l'invention.

Sur les figures qui montrent chacune schématiquement différents moyens pour réaliser l'invention, la puce électronique 10 contenant le microprocesseur de la carte comprend une unité centrale 12 et au moins une mémoire 14, par exemple du type connu sous l'acronyme anglo-saxon EEPROM FOR ELECTRICALLY ERASABLE PROGRAMMABLE READ ONLY MEMORY. Cette puce électronique présente plusieurs bornes d'entrée et/ou de sortie 16_1 à 16_8 dont l'une d'entre elles référencée 16_1 est connectée à un circuit

d'alimentation électrique 18 de tension V_{CC} tandis que celle référencée 16_5 est connectée à la masse.

Le circuit d'alimentation 18 alimente les différents éléments de la puce électronique 10 avec un courant I_{out} et, notamment, la mémoire 14 et l'unité centrale 12. Ce courant I_{out} varie en fonction des opérations effectuées par l'unité centrale et la mémoire et reflètent donc les calculs cryptographiques, ce qui pourrait permettre d'en déterminer la clé.

Pour que ce courant I_{out} ne reflète plus les opérations effectuées, l'invention propose de le modifier par un dispositif 20 ou 30, disposé dans la puce 10 et connecté, par exemple, sur la borne d'entrée 16_1.

L'invention propose de modifier le courant de deux manières différentes. Une première en faisant en sorte que le dispositif 20 (figure 1) consomme du courant de manière aléatoire ou tout au moins irrégulière, consommation supplémentaire aléatoire qui s'ajoutant à la consommation normale de courant Iin rend aléatoire la valeur I_{out}.

La deuxième manière consiste à moyenner la valeur de I_{in}, ce qui ne permet pas de détecter les variations de I_{in} dues aux opérations effectuées.

Dans le premier cas, le dispositif 20 peut être réalisé à l'aide de résistances 30, en fait des transistors, qui sont alimentées ou non selon les signaux aléatoires fournis par un générateur 28. Les courants circulant dans les résistances alimentées augmentent, modifiant la valeur du courant total et masquant le courant dû aux calculs cryptographiques.

Dans le deuxième cas, la moyenne du courant I_{in} est obtenue par un intégrateur qui "lisse" les variations du courant I_{in} de manière à les effacer.

Selon l'invention, plusieurs dispositifs 20 ou 30, référencés 20_1 et 30_1 peuvent être connectés à différents endroits de la puce électronique, par exemple, sur le conducteur d'alimentation de l'unité centrale (référence 22). En outre, ces dispositifs 20, 20_1, 30 et 30_1 peuvent être connectés ou non selon que les opérations doivent être sécurisées ou non, les connexions s'effectueront sous la commande de signaux fournis par l'unité centrale 12 (traits discontinus).

L'invention propose une troisième manière de brouiller la valeur de I_{out} en effectuant des opérations à sécuriser, telles que des calculs cryptographiques, pendant certaines phases des opérations de programmation ou d'effacement de la mémoire 14, ces opérations étant sur la commande de l'unité centrale 12.

Cette troisième manière repose sur l'utilisation d'une mémoire 14 de type EEPROM qui a la capacité d'auto-écriture.

Dans un mode habituel de fonctionnement, le microprocesseur met en marche un circuit de programmation 24 de la mémoire 14 selon les étapes suivantes :

1 - mise en marche de la pompe de charge,

2 - présentation sur le bus de données de la dernière à écrire,

3 - présentation sur le bus d'adresse de l'adresse écriture,

4 - mise en marche de la programmation,

5 - attente d'un délai de programmation,

6 - arrêt de la programmation,

7 - arrêt de la pompe de charge.

La programmation d'une cellule EEPROM nécessitant d'injecter des charges électriques dans la cellule

programmée, les étapes 4, 5 et 6 s'accompagnent d'une sur-consommation de courant d'apparence chaotique qui dépend essentiellement de la valeur de V_{CC}, de l'adresse, de la valeur programmée et de la température du composant.

Afin de masquer l'empreinte de consommation de courant d'un calcul cryptographique par exemple, l'invention propose d'utiliser la consommation chaotique des étapes 4, 5 et 6 en réalisant le calcul cryptographique pendant l'étape 5 d'une durée de quelques millisecondes.

Pour ce faire, le calcul cryptographique s'effectue selon les étapes suivantes :

1 - mise en marche de la pompe de charge,

2 - présentation sur le bus de données d'une donnée aléatoire,

3 - présentation sur le bus d'adresse d'une adresse écriture,

4 - mise en marche de la programmation,

5 - effectuer le calcul cryptographique,

6 - arrêt de la programmation,

7 - arrêt de la pompe à charge.

Par ces étapes, l'empreinte de la consommation de courant due au calcul cryptographique de l'étape 5 est masquée par l'écriture de la donnée aléatoire dans une partie déterminée 26 de la mémoire EEPROM réservée à cette fonction.

Au lieu d'un calcul cryptographique, l'étape 5 peut consister en toute opération à sécuriser vis-à-vis de l'extérieur.

Par ailleurs, au lieu de faire ces opérations à sécuriser lors d'une écriture dans la mémoire 14, elles peuvent être faites lors d'un effacement de la mémoire 14.

REVENDICATIONS

1. Dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce à microprocesseur, caractérisé en ce qu'il comprend au moins un moyen (20, 30, 28, 26) pour modifier la consommation de courant dudit composant lors de la réalisation desdites opérations.

2. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un circuit intégrateur (30) du courant du composant de manière à moyenner les variations de ce courant au cours du temps.

3. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant comprend au moins un générateur (28) de signaux aléatoires et une batterie de résistances (20) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires.

4. Dispositif selon la revendication 1, caractérisé en ce qu'il comprend une pluralité de moyens (20, 20_1, 30, 30_1) pour modifier la consommation de courant.

5. Dispositif selon la revendication 1, caractérisé en ce que le moyen pour modifier la consommation de courant du composant dans le cas d'une mémoire (14) du type EEPROM, associée à une unité centrale (12) du microprocesseur, comprend un moyen pour effectuer simultanément une opération d'écriture ou d'effacement

d'une mémoire (14) dite de masquage et une opération du microprocesseur.

6. Dispositif selon la revendication 5, caractérisé en ce que, pour mettre en oeuvre une opération d'écriture ou d'effacement dite de masquage, la mémoire (14) comprend une partie (26) dédiée à l'enregistrement d'une donnée aléatoire.

7. Dispositif selon l'une des revendications 1 à 6, caractérisé en ce qu'il comprend, en outre, un moyen de mise en route de chacun des moyens de modification de la consommation de courant à chaque opération à sécuriser.

8. Procédé pour mettre en oeuvre le dispositif selon la revendication 5 ou 6, caractérisé en ce que, dans le cas d'un calcul cryptographique, il comprend les étapes suivantes consistant à :

- mettre en marche la pompe de charge,
- présenter une donnée aléatoire sur le bus de données,
- présenter une adresse d'écriture sur le bus d'adresses,
- mettre en marche la programmation,
- effectuer le calcul cryptographique,
- arrêter la programmation, et
- arrêter la pompe de charge.

9. Procédé pour masquer les opérations effectuées par un composant, caractérisé en ce qu'il comporte les étapes suivantes :

- mise en marche de la pompe de charge,
- présentation sur le bus de données d'une donnée aléatoire,

- présentation sur le bus d'adresses d'une adresse d'écriture,
- mise en marche de la programmation,
- réalisation du calcul cryptographique,
- arrêt de la programmation, et
- arrêt de la pompe de charge.

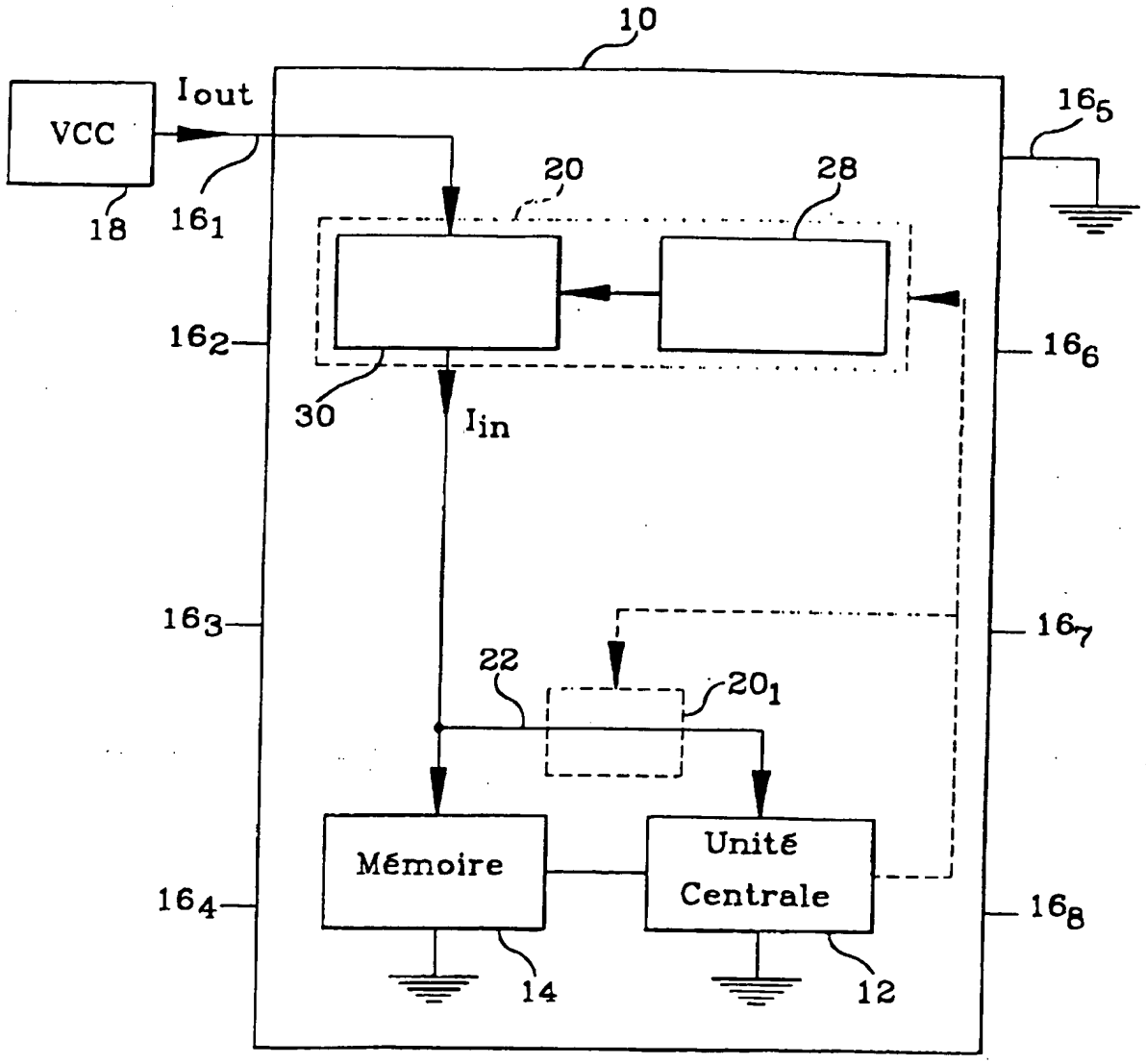


FIG.1

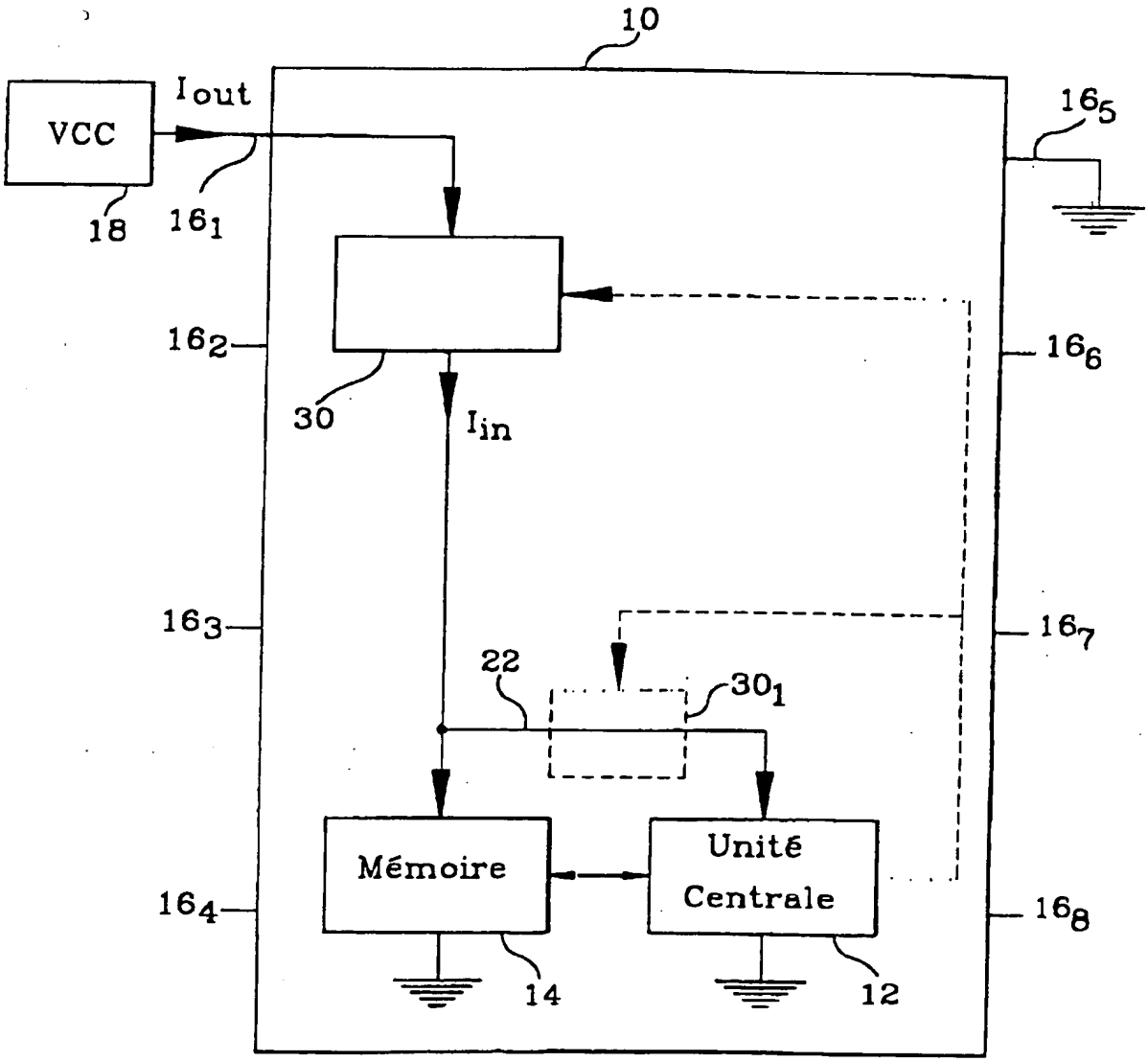


FIG.2

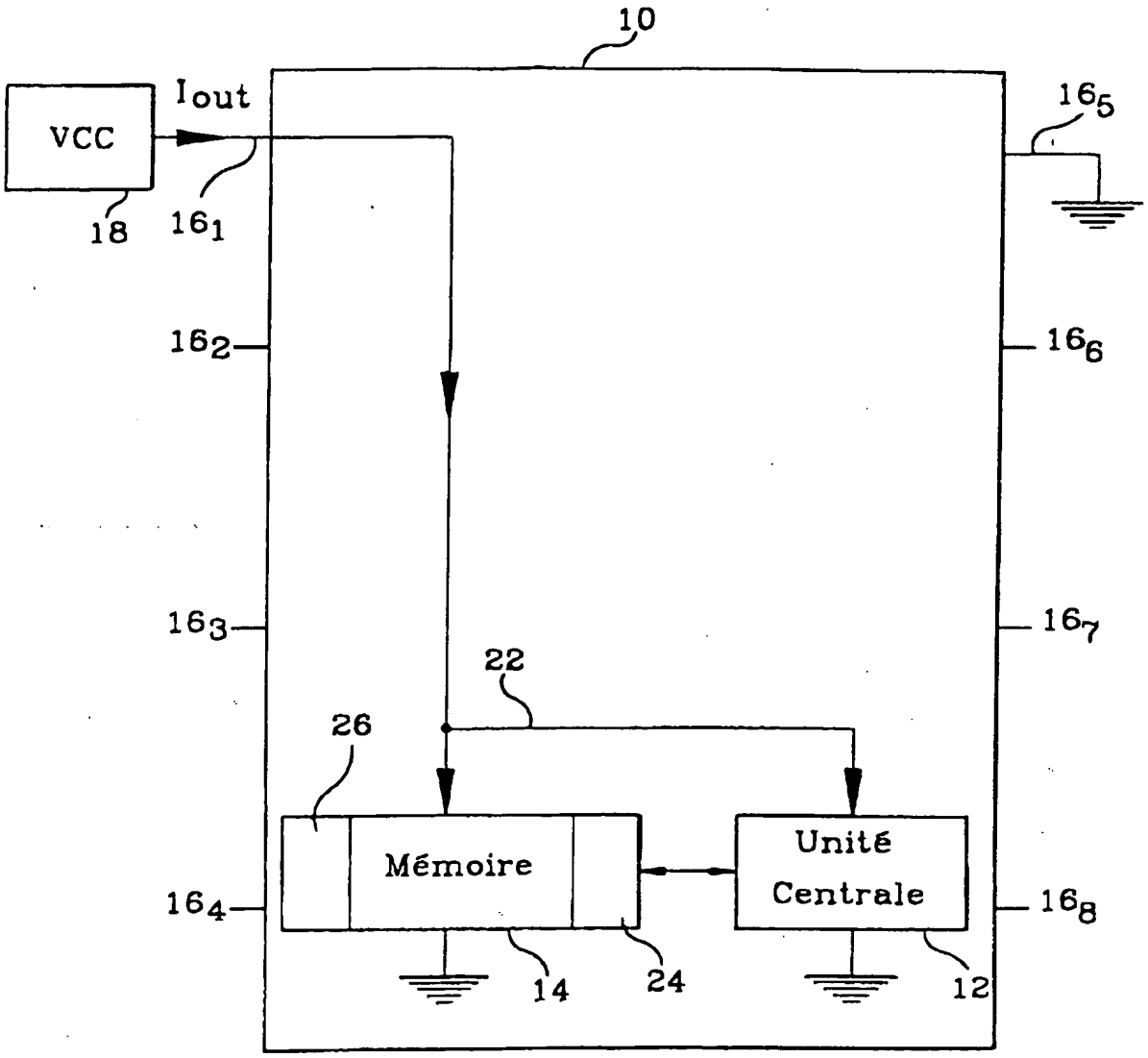


FIG.3

2776410

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 562778
FR 9803471

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
X	US 4 295 041 A (UGON MICHEL) 13 octobre 1981 * abrégé; revendication 1; figures 1,2 * * colonne 1, ligne 61 - colonne 2, ligne 21 *	1,5,7
X Y	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 juin 1990 * abrégé; figure 4 * * colonne 2, ligne 29-59 * * colonne 3, ligne 26 - colonne 4, ligne 21 *	1,3,4,7 6
X Y	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 mars 1989 * colonne 2, ligne 8-31 * * colonne 3, ligne 63 - colonne 4, ligne 13 * * colonne 6, ligne 18-22 *	1,5,7 6,8,9
Y	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996 * page 1, ligne 5-20 * * page 2, ligne 3-10 * * page 13, ligne 8-20 * * page 22, ligne 9-18 *	8,9

DOMAINES TECHNIQUES RECHERCHES (Int.CL.6)

G07F
G06K
G06F

1

Date d'achèvement de la recherche: 15 décembre 1998

Examinateur: Cardigos dos Reis, F

EPO FORM 1503 03.82 (P04C13)

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant